



Legislative Audit Division

State of Montana

Report to the Legislature

February 2005

Information System Audit

Automated Licensing System (ALS)

Department of Fish, Wildlife and Parks

This report contains two recommendations addressing:

- ▶ **Excessive access privileges for ALS users.**
- ▶ **Documentation for manual license revenue collection procedures.**

**Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705**

05DP-03

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator John Cobb
Senator Mike Cooney
Senator Jim Elliott, Acting Chair
Senator John Esp
Senator Dan Harrington
Senator Corey Stapleton

Representative Dee Brown
Representative Tim Callahan
Representative Hal Jacobson
Representative Scott Mendenhall
Representative John Musgrove
Representative Rick Ripley

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel



Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

February 2005

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of the Automated Licensing System (ALS) operated by the Department of Fish, Wildlife and Parks. Our audit focused on the effectiveness of controls over user access, the license drawing process, and the license revenue collection process as well as the accuracy of license fee amounts.

The report contains one recommendation regarding excessive user access privileges, and one recommendation regarding documentation for manual license sweep procedures.

We wish to express our appreciation to the department for their cooperation and assistance.

Respectfully submitted,

(Signature on File)

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

Information System Audit

Automated Licensing System (ALS)

Department of Fish, Wildlife and Parks

Members of the audit staff involved in this audit were David P. Nowacki and Dale Stout.

Table of Contents

| | |
|--|------------|
| Appointed and Administrative Officials | ii |
| Executive Summary | S-1 |
| Chapter I - Introduction..... | 1 |
| Introduction and Background | 1 |
| Objectives | 2 |
| Audit Scope and Methodology | 2 |
| Summary and Conclusions | 3 |
| Chapter II - User Access..... | 5 |
| Introduction..... | 5 |
| Excessive Access Privileges | 5 |
| Chapter III - Revenue Collection Procedures | 9 |
| Introduction..... | 9 |
| Procedures Not Documented and No Trained Backup | 9 |
| Department Response | A-1 |
| Department of Fish, Wildlife and Parks | A-3 |

Appointed and Administrative Officials

Department of Fish, Wildlife and Parks

Jeff Hagener, Director

Chris Smith, Chief of Staff

Barney Benkelman, Information Technology Bureau Chief

Fish, Wildlife and Parks Commission

| | <u>City</u> | <u>Term Expires</u> |
|-------------------------|-------------|---------------------|
| Steve Doherty, Chairman | Great Falls | 2009 |
| Tim Mulligan | Whitehall | 2007 |
| Victor Workman | Whitefish | 2009 |
| John Brenden | Scobey | 2007 |
| Shane Colton | Billings | 2009 |

Executive Summary

The Department of Fish, Wildlife and Parks (FWP) operates the Automated Licensing System (ALS) to support licensing operations. System implementation began in 2002 and was completed in 2004. In 2002, we performed a limited scope audit of ALS operations (02DP-07) in support of financial compliance auditors.

The scope of this audit was comprised of four primary objective areas including: determining whether access controls exist to prevent excessive user access privileges, determining whether license fee amounts are accurate according to state law, determining whether the drawing process controls facilitate a random drawing, and determining whether controls exist over the license revenue collection process. Audit work included interviews and observations with FWP personnel, review of reports for appropriateness of user access and accuracy of license fee amounts, and analysis of data generated by the random drawing process to verify that was random.

We determined that license fee amounts in the ALS database were accurate and that each license drawing application entry has an equal chance of being selected. We also determined that excessive user access privileges exist in the database, and that documentation and back-up procedures are lacking in the license revenue collection process. These issues are discussed in chapters two and three.

Chapter I - Introduction

Introduction and Background

The Automated Licensing System (ALS) automates the Department of Fish, Wildlife, and Parks (FWP) hunting, fishing, and recreational license issuance process including special licenses and permits. ALS also aides FWP in conducting license drawings and supports administrative business functions related to licensing.

Licensee information such as name, address, social security number and other identifying information, as well as a record of licenses purchased, is stored in the database. This data is used by wardens for enforcement purposes and also used in reporting to state and federal agencies. License fee amounts, accounting codes, and inventory data is also maintained in the database. This data aids providers in charging licensees proper license amounts and allows for FWP to collect license revenue from providers and pay commissions to providers based on license sales through the revenue collection process. In fiscal year 2004 approximately \$37 million in license fee revenue was processed on the system.

The system issues licenses and permits using point-of-sale (POS) terminals at license provider locations that communicate with servers housed and maintained by the State of Montana's Information Technology Services Division (ITSD). ALS users include FWP employees and contractors who develop and administer ALS, internal FWP providers who issue licenses at FWP headquarters and regional offices, external license retailers who issue licenses from their business locations, and public users who access ALS from the web. Special licenses and permits for restricted areas and time periods are available through a drawing process that is performed by FWP personnel using data from ALS. System implementation began in 2002 and was completed during 2004. Current development efforts consist of system improvements and enhancements. We conducted an audit of ALS in 2002 (02DP-07), when a limited number of licenses were maintained in ALS. Currently, ALS maintains all licenses and permits issued by FWP.

Chapter I - Introduction

Objectives

We conducted a comprehensive review of ALS operations and our primary objectives included:

- ▶ **Determining whether access controls exist to prevent excessive user access privileges:** Data integrity depends on the appropriateness of users having the ability to change data, and whether privileges are necessary.
- ▶ **Determining whether license fee amounts are accurate according to state law:** The proper charging of license fee amounts by providers depends on the accuracy of license fee amounts in the database.
- ▶ **Determining whether the drawing process controls facilitate a random drawing:** It is important that the public perceives the license drawing process as random.
- ▶ **Determining whether controls exist over the license revenue collection process:** The collection of revenue from license providers depends on the accuracy of license fee amounts and the controls over the revenue collection process.

Audit Scope and Methodology

Areas of ALS operations are the responsibility of ITSD or contractors as defined in service level agreements and contractual language. The audit scope included only areas of the ALS application, hardware, and operations as managed by FWP personnel. These areas include user access configuration, management of the license fee amounts and data within the database, the special license drawing process, and the revenue collection process. Audit work included interviews and observations with FWP, review of reports for appropriateness of user access and accuracy of license fee amounts, and analysis of data generated by the random drawing process to verify that it was random.

Criteria we used to evaluate objective areas included state law, the Information Systems Audit and Control Association's Control Objectives for Information Technology, information technology industry accepted practices, and FWP regulations. The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office (GAO).

Summary and Conclusions

The collection of license revenue depends on license fee amounts in the database being accurate in accordance with state law. We confirmed that all license fee amounts in the database were accurate. Additionally, FWP represents to the public that the license drawing process is ‘completely random’, further stating that the random number is the only connection between the drawing and the applicant. We analyzed random number generator output and confirmed that it produced random numbers. Each drawing application entry has an equal chance of being selected.

We reviewed the controls over the process to grant user access to the ALS administrative application screens. There is no documented process to grant users access, and issues were noted regarding excessive privileges granted to users. We also reviewed controls over the license revenue collection process. Overall, this process is controlled, except for an issue regarding lack of documented procedures or trained backup personnel. These issues are discussed in the following chapters.

Chapter II - User Access

Introduction

There are two primary user interfaces from which users can access the ALS database. One is the point of sale (POS) application, which is used by license providers to issue licenses and enter licensee information. The other is the administrative application, which is used by FWP employees and contractors for maintaining and administering the database. Examples of administrative and maintenance activities include changing accounting codes, license fee amounts, and licensee information. Users can also access the database directly without using either application.

FWP employee user access requests are communicated via phone or email, not by approved forms. Administrative users are granted access to the database through the administrative application screens or directly through the database. ALS providers are granted access to the POS device screens through the POS application screens, and responsibility for controlling access is delegated to the providers. For direct database access and access to administrative application screens, control of access is the responsibility of ALS Operations personnel.

Excessive Access Privileges

We reviewed access privileges for the administrative application granted to select department administrators, licensing personnel, operations personnel, development personnel, and contractors. For the six users examined, access was identified that was unnecessary to fulfill the users' job functions. We confirmed the unnecessary access with the ALS personnel, who acknowledged the problem and stated that access needed to be "cleaned up". Personnel indicated that the user portion of the production database was probably copied over from the development database when they went live in 2002.

Industry standards state that management should implement procedures that provide access security control based on the individual's demonstrated need to add, change, or delete data, and should have a control process in place to review and confirm access rights periodically via periodic comparisons with recorded accountability.

Chapter II - User Access

Unnecessary access to system screens and data enable a user to perform functions not related to job duties. Users can access and change data either accidentally or intentionally. The procedures to grant user access to the administrative application are not documented. No periodic review of user access privileges for appropriateness is performed, which would facilitate the identification and removal of inappropriate user access. During our fieldwork, ALS personnel could not trace 3 contractor User ID's back to an actual contractor.

Additionally, when a new user is created in the administrative application, the user is given, by default, excessive privileges for the underlying tables in the ALS production database. Users who directly access the database outside of the administrative application have the ability to insert, update, and delete any ALS data in the database. FWP personnel stated this was a design decision made for the sake of simplicity, and no second thought was ever given to changing it until now. ALS personnel recognized the issue's significance and worked to develop a fix, which they indicated was implemented by the end of calendar year 2004.

Activity logs are generated daily and reviewed several times per week. The database administrator reviews the logs manually and searches for logins outside normal business hours, excessive failed login attempts, logins with non-standard software, and other irregular events. Monitoring efforts only keep track of when a user logs in and not what actions are performed while accessing the system; therefore, changes made to data in the production database could go unnoticed.

Recommendation #1

We recommend FWP:

- A. Develop and maintain written procedures for granting user access to ALS, and**
- B. Periodically review user access for appropriateness.**

Chapter III - Revenue Collection Procedures

Introduction

The billing period for license providers is seven days starting each Friday and ending each Thursday. The license revenue collection process occurs for each billing period, and includes the collection of license fee amounts from provider bank accounts and payment of commissions based on license sales. License providers authorize and designate a bank account to be used in the revenue collection process when they become providers. Included in this cycle is the creation of a remittance report notifying license providers the amount of funds to have in their bank account for collection, and manual procedures performed by licensing bureau personnel to reconcile the collection totals and create SABHRS and ALS accounting entries. A revenue collection file is manually sent via File Transfer Protocol (FTP) to an Automated Clearing House, where funds are collected from provider bank accounts. Manual procedures are also necessary when a failed collection from a provider account occurs, requiring the failed revenue collection file to be uploaded back into ALS and notifications to be sent to the provider.

Procedures Not Documented and No Trained Backup

With the exception of the revenue collection file reconciliation, which is done by two employees, a single licensing bureau employee performs the majority of the manual procedures during the license revenue collection process. The procedures performed are not documented and there are no trained backup personnel to mitigate the risk presented by not having documented procedures. Industry standards state that management should establish and document standard procedures for operations. FWP estimates that it collects an average of \$400,000 per week through the revenue collection process. In the event that this employee becomes unable to perform his/her job duties, the revenue collection process could be delayed. Management has not addressed the risks associated with long-term loss of key personnel. For example, management considered training backup personnel in case of an absence, but instead decided to wait until the employee returned to work.

Chapter III – Revenue Collection Procedures

Recommendation #2

We recommend FWP:

- A. Document procedures performed during ALS license revenue collection process, and**
- B. Train backup personnel to perform duties in case of absence.**

Department Response



Montana Fish, Wildlife & Parks

RECEIVED

MAR 02 2005

LEGISLATIVE AUDIT DIV.

P.O. Box 200701
Helena, MT 59620-0701
(406) 444-3186
FAX: 406-444-4952
Ref: DO0078-05
February 28, 2005

David Nowacki
Senior IS Auditor
State Capitol Room 160
PO Box 201705
Helena, MT 59620-1705

Dear Mr. Nowacki:

Montana Fish, Wildlife & Parks' (FWP) has reviewed the most recent audit report issued on the Automated Licensing System (ALS). FWP's response to the two recommendations follow. For convenience, FWP has excerpted each recommendation, and FWP's response follows each.

Recommendation #1

We recommend that FWP:

- A. Develop and maintain written procedures for granting user access to ALS and,**
- B. Periodically review user access for appropriateness.**

Response:

Concur.

During the audit FWP was in the process of developing ALS access request forms. As well, during audit discussions, it was recognized that some users carried the same access that existed in the development environment into the production environment. This conversion had been done for convenience during the heavy workload of full-scale implementation, and had simply not been re-addressed. It has now been reviewed and corrected. As the first large scale automated system developed, managed and supported by FWP, staff continue to learn of unanticipated support requirements as full use of ALS brings them to light. As noted during the audit, FWP staff already performed reviews of access to ALS on a regular basis, but had not yet established a formal practice of review that examined level of detail desired by Audit staff. Both issues can be attributed to workload. It is understood that both areas need further detailed refinement, and formal documents and procedures need to be documented and integrated into full operation.

- A. At this writing, the request form for external users has been completed and has been modified to provide for internal users. In addition "procedures" for requesting access

have been drafted. Copies are attached for your review. These documents will continue to be refined as actual use identifies additional areas that are not adequately met with these forms and procedures.

- B. FWP has a Decision Package before the Executive Budget Committee that, if approved, will allow a specific staff member to be dedicated to “security”. This staff member will be responsible for providing and monitoring access to all FWP applications, including ALS. Over the next year, it is anticipated that increasingly detailed review procedures will be developed, refined and executed to include the less obvious methods of potential intrusion.

Recommendation #2

- A. Document procedures performed during ALS license revenue collection process and,
- B. Train backup personnel to perform duties in case of absence.

Response:

Concur.

At the time of the audit, procedures already existed but were not in a form that were easily isolated or used by staff unfamiliar with the process. These instructions continue to be refined with the expectation that the final product will be easy to understand and used by additional Licensing staff.

- A. The initial draft is being provided for your review and will continue to be refined to provide an easy to follow set of rules to accomplish the revenue collection (Electronic Funds Transfer – EFT) process
- B. Backup staff have been identified so that in the event of planned or unplanned absences, FWP will be capable of continuity in the collection process.

FWP appreciates the opportunity to respond to these recommendations, and the professional manner in which the audit was conducted.

Sincerely,



M. Jeff Hagener
Director

Encs.